A construction of 3-e.c. graphs using quadrances

Le Anh Vinh
Mathematics Department
Harvard University
Cambridge, MA 02138, US
vinh@math.harvard.edu

March 13, 2009

Abstract

A graph is n-e.c. (n-existentially closed) if for every pair of subsets A, B of vertex set V of the graph such that $A \cap B = \emptyset$ and $|A| + |B| = n$, there is a vertex z not in $A \cup B$ joined to each vertex of A and no vertex of B. Few explicit families of n-e.c. are known for $n > 2$. In this short note, we give a new construction of 3-e.c. graphs using the notion of quadrance in the finite Euclidean space $\mathbb{Z}_p^d$.

1 Introduction

For a positive integer n, a graph is *n-existentially closed* or n-e.c. if we can extend all n-subsets of vertices in all possible ways. Precisely, if for every pair of subsets A, B of vertex set V of the graph such that $A \cap B = \emptyset$ and $|A| + |B| = n$, there is a vertex z not in $A \cup B$ joined to each vertex of A and no vertex of B. From the results of Erdös and Rényi [2], almost all finite graphs are n-e.c. Despite this result, until recently, only few explicit examples of n-e.c. graphs are known for $n > 2$ (see [1] for a comprehensive survey on the constructions of n-e.c. graphs). In this short note, we give a new construction of 3-e.c. graphs using the notion of quadrance in the finite Euclidean space $\mathbb{Z}_p^d$.

Suppose that p be an odd prime, and that $\mathbb{Z}_p = \{0, \ldots, p-1\}$ be the prime field with p elements. We will construct a 3-e.c. graph with the vertex set $\mathbb{Z}_p^d$ for some large d. The following definition of quadrance is taken from [4].

Definition 1.1 *The quadrance between the points $X = (x_1, \ldots, x_d)$ and $Y(y_1, \ldots, y_d)$ in $\mathbb{Z}_p^d$ is the number*

$$Q(X,Y) := (x_1 - y_1)^2 + \ldots + (x_d - y_d)^2 \in \mathbb{Z}_p.$$

Let $V_1 = \{0, 1, 2, \ldots, (p-1)/2\}$. We define the graph $G_{p,d}$ as follows. The vertices of the graph $G_{p,d}$ are the points of $\mathbb{Z}_p^d$. There is an edge between two vertices X and Y if and only if $Q(X,Y) \in V_1$. We claim that $G_{p,d}$ is 3-e.c. for $p \geqslant 7$ and $d \geqslant 5$.

Theorem 1.2 *Suppose that $p \geqslant 7$ be an odd prime and $d \geqslant 5$ be an integer. Then the graph $G_{p,d}$ is 3-e.c.*

Note that these quadrance graphs are just Cayley graphs of $\mathbb{Z}_p^d$.

2 The 3-e.c. property of the graph $G_{p,d}$

We now give a proof of Theorem 1.2. Let $V_2 = \{(p+1)/2 \ldots, p-1\} = \mathbb{Z}_p \backslash V_1$. It suffices to show that for any three distinct points $A = (a_1, \ldots, a_d)$, $B = (b_1, \ldots, b_d)$, $C = (c_1, \ldots, c_d)$ in $\mathbb{Z}_p^d$ and $i, j, k \in \{1, 2\}$, there is a point $X = (x_1, \ldots, x_d) \in \mathbb{Z}_p^d$, $X \neq A, B, C$ such that $Q(X, A) \in V_i$, $Q(X, B) \in V_j$ and $Q(X, C) \in V_k$. Therefore, we only need to show that there exist $u \in V_i, v \in V_j$, and $w \in V_k$ such that the following system has at least four solutions (in this case, one of these solutions is different from A, B, and C),

$$
\begin{aligned}
(x_1 - a_1)^2 + \ldots + (x_d - a_d)^2 &= u \qquad (2.1)\\
(x_1 - b_1)^2 + \ldots + (x_d - b_d)^2 &= v \qquad (2.2)\\
(x_1 - c_1)^2 + \ldots + (x_d - c_d)^2 &= w. \qquad (2.3)
\end{aligned}
$$

For any $X = (x_1, \ldots, x_d) \in \mathbb{Z}_p^d$, define

$$\|X\| = x_1^2 + \ldots + x_d^2.$$

By eliminating x_i^2's from (2.2) and (2.3), we get an equivalent system of equations

$$
\begin{aligned}
Q(X, A) &= u \qquad (2.4)\\
\langle X, B - A \rangle &= (u - v + \|B\| - \|A\|)/2 \qquad (2.5)\\
\langle X, C - A \rangle &= (u - w + \|C\| - \|A\|)/2. \qquad (2.6)
\end{aligned}
$$

We first show that the system of two equations (2.5) and (2.6) has a solution X_0 for some choices of $u \in V_i$, $v \in V_j$, and $w \in V_k$. We consider two cases.

Case 1. Suppose that $B - A$ and $C - A$ are linearly independent. For any $u \in V_i$, $v \in V_j$, and $w \in V_k$, it is clear that there is a solution X_0 to the system of two equations (2.5) and (2.6).

Case 2. Suppose that $B - A$ and $C - A$ are linearly dependent. Since $C - A \neq B - A \neq 0$, $C - A = t(B - A)$ for some $t \neq 0, 1$. The two equations (2.5) and (2.6) have a common solution if we can choose $u \in V_i$, $v \in V_j$, and $w \in V_k$ such that

$$u - w + \|C\| - \|A\| = t(u - v + \|B\| - \|A\|),$$

or equivalently,

$$w = tv + a,$$

where $a = \|C\| + (t - 1)\|A\| - t\|B\| - (t - 1)u$. In other words, we need to show that $\{tv : v \in V_j\} \cap \{w - a : w \in V_k\} \neq \emptyset$. We have two subcases.

- Suppose that $t \neq 0, \pm 1$. We label $\mathbb{Z}_p$ around the circle. The set $\{w - a : w \in V_k\}$ is a block of $(p \pm 1)/2$ consecutive points. Going $|V_k| = (p \pm 1)/2$ steps of length $2 < |t| \leqslant (p-1)/2$ around the circle, we cannot avoid any block of $(p \pm 1)/2$ consecutive points. Hence, for any fixed $u \in V_i$, we can choose $v \in V_j$ and $w \in V_k$ such that $w = tv + a$.

- Suppose that $t = -1$. The set $\{w + v : w \in V_k, v \in V_j\}$ contains at least $p - 2$ elements. Since $|A_i| \geqslant (p-1)/2 \geqslant 3$, we can choose u such that $a \in \{w + v : w \in V_k, v \in V_j\}$.

Therefore, we always can choose $u \in V_i$, $v \in V_j$, and $w \in V_k$ such that the two equations (2.5) and (2.6) have a common solution X_0.

Take a basis of solutions of the system

$$\begin{aligned} \langle X, B - A \rangle &= 0 \\ \langle X, C - A \rangle &= 0, \end{aligned}$$

and the solution X_0. Substitute them into (2.4), we get a single quadratic equation of $d - 2$ variables. Since $d - 2 \geqslant 3$, this quadratic equation has at least p (≥ 4) solutions. Theorem 1.2 follows immediately.

3 Remarks and Further Questions

Note that the construction is well defined over $\mathbb{Z}_m$ for any $m \in \mathbb{N}$ and it gives 3-e.c. graphs as well. The proof goes without any essential changes when p is not a prime.

Moreover, the proof of Theorem 1.2 only works for $d \geq 5$. It is plausible to conjecture that the graphs are 3-e.c. for $d \geq 2$. Another interesting question is to consider other constructions with difference choices of $V_1 \subset \mathbb{Z}_p$. When $d = 2$, let $V = \{a^2 : a \in \mathbb{Z}_p^*\}$. We define the graph $G_{V,p}$ as follows. The vertices of the graph $G_{V,p}$ are the points of $\mathbb{Z}_p^2$. There is an edge between two vertices X and Y if and only if $Q(X, Y) \in V$. We know that $G_{V,p}$ is isomorphic to the Paley graph P_p (see, for example, [3]). It is well known that P_p is n-e.c for any n given that p is sufficiently large, so is $G_{V,p}$. We, however, have not known any results for the remaining cases.

Acknowledgment

The author would like to thank Prof. Igor Shparlinski for helpful advice on the proof of Theorem 1.2. He also wants to thank the referee for constructive comments and suggestions.

References

[1] A. Bonato, The search for n-e.c. graphs, *Contributions to Discrete Mathematics*, to appear.

[2] P. Erdös and A. Rényi, Asymmetric graphs, *Acta Math. Acad. Sci. Hungar.* **14** (1963) 295–315.

[3] L. A. Vinh, Quadrance graphs, *Aus Math Soc GAZETTE*, **33** (5), 2006, 330–332.

[4] N. J. Wildberger, *Divine Proportions: Rational Trigonometry to Universal Geometry*, Wild Egg Books, Sydney 2005.